In preparing a Privacy Impact Assessment (PIA), the Program Manager for the Information Technology (IT) investment should follow the October 28, 2005 Department of Defense (DoD) format - http://www.defenselink.mil/cio-nii/docs/DoD_PIA_Guidance_Oct_28_2005.pdf (which supersedes section A4E, paragraph A4.9 on pages 58-61 of AFI 33-332 in http://www.e-publishing.af.mil/pubfiles/af/33/afi33-332/afi33-332.pdf) by completing the 21 questions below. The Program Manager should collaborate with the IT personnel for the investment (programmers, developers, database administrators, etc) as well as the Portfolio Manager and Privacy Act Official. Instructions for the 21 questions are adapted from "DLA PIA Template and Instructions" at http://www.dla.mil/public_info/efoia/PIA.html .

The Portfolio Managers are listed by Major Command (MAJCOM), Direct Reporting Unit (DRU), or Field Operating Agency (FOA).in the Air Force Portal – after logging into https://www.my.af.mil/ , click "Application A-Z Listing", click the "E", click to scroll down to "EITDR", click "PfM PoC List", click "EITDR PFM LISTING").

Contact your base Privacy Act Office.

Attachment 2

DoD Privacy Impact Assessment (PIA) format

(Use N/A where appropriate or write "Not applicable")

Spell out any acronyms. After it has been spelled out, the acronym can used in the remainder of the Privacy Impact Assessment.

Remember, the intended audience is the general public.

1. Department of Defense (DoD) Component.
*** United States Air Force*

2. Name of Information Technology (IT) System.
*** Provide the full name of your IT investment as reported in the (Enterprise Information Technology Data Repository (EITDR) at https://www.my.af.mil/eitdrprod via the Air Force Portal at http://www.my.af.mil) or on your Federal Information Security Management Act of 2002 (FISMA) report.*

3. Budget System Identification Number (SNAP-IT Initiative Number).
- the portfolio's number assigned by SNAP-IT, which is a repository for Capital Investment Reporting (CIR), Selected Capital Investment Reporting (SCIR), and Exhibit 53 data. Exhibit 53 data is an electronically-submitted, format-consistent form required by the Office of Management and Budget (OMB) for capital investment requests. The Budget System Identification Number replaced the AF- and DoD-ITMA (Information Technology Management Application) number.

*** This is the "BIN" number at the upper right area of EITDR for your investment. Or write "not applicable".*

4. System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR)).

- the portfolio's number assigned by the DoD Information Technology Portfolio Repository (DITPR)

*** This is the "DITPR" number given at the upper right area of EITDR for your investment. Or write "not applicable".*

5. IT Investment (OMB Circular A-11) Unique Identifier (if applicable).

- 2007 Unique Project Identifier (UPI) means the unique project identifier used to report the investment in the 2007 Budget. As agencies capital planning processes mature and investments are aligned to the Federal Enterprise Architecture (FEA), the unique project identifiers should be changed to match the appropriate FEA Mappings. Indicating the UPI used for the 2007 Budget process allows cross-walk and historical analysis crossing fiscal years for tracking purposes.
- 2008 UPI means the identifier depicting agency code, bureau code, mission area (where appropriate), part of the exhibit where investment will be reported, type of investment, agency four-digit identifier, and two-digit investment category code.

*** This is the number given at EITDR question G11 for your investment. Or write "not applicable".*

6. Privacy Act System of Records Notice Identifier (if applicable).

- identifies the applicable Privacy Act system of records notice.

*** Air Force Privacy Act systems of records notices (SORNs) are found at http://www.defenselink.mil/privacy/notices/usaf/ . The primary DoD webpage for SORNs is http://www.defenselink.mil/privacy/notices/ . Or write "not applicable".*

7. OMB Information Collection Requirement Number (if applicable) and Expiration Date.

- Part 1320 of Title 5, Code of Federal Regulations (Reference (g)) at http://www.access.gpo.gov/nara/cfr/waisidx_07/5cfr1320_07.html directs that public information collections be submitted to the Office of Management and Budget (OMB) for approval and assigned an OMB control number.

*** Provide the OMB Control Numbers, expiration dates, and titles of any information collection requests (e.g. forms, surveys, etc.) contained in the IT investment and approved by OMB under the Paperwork Reduction Act (PRA) - http://www.dtic.mil/whs/directives/corres/pdf/891001p.pdf .*

Are any forms being used to collect data for your IT investment? If yes, what is the form number, and what is the OMB authorization and expiration? The AF forms website is located at http://www.e-publishing.af.mil/orgs.asp?type=forms ; links to other websites with forms are also listed. If the forms used do not have any OMB information, write "not applicable".

For example, the Defense Finance and Accounting Service (DFAS) at http://www.dfas.mil/more/dfasfreedomofinformationactprivacyact/dfaspia.html has a

Privacy Impact Assessment for the "Defense Debt Management System (DDMS)". Item 7 for the DDMS Privacy Impact Assessment has "DD Form 2789, Waiver/Remission of Indebtedness Application, OMB No. 0730-0009, OMB approval expires November 30, 2008." At the DD forms website (http://www.dtic.mil/whs/directives/infomgt/forms/ddforms2500-2999.htm) for DD Form 2789, the OMB information appears at the upper right area of the form (http://www.dtic.mil/whs/directives/infomgt/forms/eforms/dd2789.pdf).
Or write "not applicable".

8. Type of authority to collect information (statutory or otherwise).
*** What specific authorities, arrangements, and/or agreements define the collection of the data in the IT investment? Include the authorities to collect the Privacy Act data, if applicable.*
Be consistent with what you have written in the System of Record Notice for your IT investment. AF SORNs are listed at http://www.defenselink.mil/privacy/notices/usaf/ .

9. Provide a brief summary or overview of the IT system (activity/purpose, present lifecycle phase, system owner, system boundaries and interconnections, location of system and components, and system backup).
*** Provide information on what the investment does, who it serves, the office that owns the IT investment, point of contact name, telephone number, email, etc. Length of this entry will depend on the size and complexity of the IT investment and its subsystems, where relevant.*

10. Describe what information in identifiable form will be collected and the nature and source of the information (e.g. names, Social Security Numbers, gender, race, other component IT systems, IT systems from agencies outside DoD, etc.).
*** List the identifiable information being collected and its source.*

11. Describe how the information will be collected (e.g., via the Web, via paper-based collection, etc.).
*** Address how you are collecting the information (via the web, via paper-based collection, via exchanges from other data systems, etc) from the subject individual or other sources, etc. Describe why information from "other sources" is required.*

12. Describe the requirement and why the information in identifiable form is to be collected (e.g., to discharge a statutory mandate, to execute a Component program, etc.).
*** Describe why the personally identifiable information collected and stored in the IT investment is necessary to the AF/DoD mission, e.g. to discharge a statutory mandate, to execute a Component program, to verify an individual's identity, etc.*

13. Describe how the information in identifiable form will be used (e.g., to verify existing data, etc.).

*** Identify and list each use (internal and external to AF/DoD) of the personally identifiable information collected and maintained. If a Privacy Act system of records notice exists, summarize the most relevant uses/routine uses.*

14. Describe whether the system derives or creates new data about individuals through aggregation.

*** Describe if the investment creates or makes available new or previously unavailable information about an individual, state/explain what will be done with the newly derived information, i.e. collect multiple pieces of personally identifiable information data from various sources on an individual, thereby creating a new data profile for that person.*

15. Describe with whom the information in identifiable form will be shared, both within the Component and outside the Component (e.g., other DoD Components, Federal agencies, etc.).

*** Internal to AF - Describe with whom the information will be shared within AF/DoD and uses made of the data. All individuals accessing information contained in an IT investment or a Privacy Act system of records are to have taken Information Assurance and Privacy Act training, and thus made aware of the consequences of inappropriately using information contained therein.*

*** External to AF - Describe with whom the information will be shared outside the DoD. Where a specific authority exists to share the information, please provide the authority citation. If a Privacy Act system of records is involved with the IT investment, the data may also be provided under any of the routine uses published in the system of records notice and/or the DoD "Blanket Routine Uses" published at http://www.defenselink.mil/privacy/notices/blanket-uses.html , if applicable.*

16. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent.

*** Can the individual refuse to provide personally identifiable information for this IT investment?*

Example:

-- All personal data collected is voluntarily given by the subject individual. Forms that collect personal data to be maintained in this IT investment contain a Privacy Act Statement, as required by 5 U.S.C. 552a(e)(3) at http://uscode.house.gov/download/pls/Title_05.txt , allowing the individual to make an informed decision about providing the data. The statement advises the individual that the information provided is voluntary and provides the consequences of choosing not to participate with the information collection. Individuals may raise an objection with the Air Force Privacy Act office during the public comment period of the Privacy Act system of records notice (if applicable) or during the data collection.

-- The subject individual initiates the collection and maintenance of his/her information for the purpose of [insert purpose]. Release of this information is done with the individual's full cooperation and consent.

-- Data is provided by other Federal agencies, State and local government organizations, and private sector entities. Information may also be purchased from commercial databases for inclusion in this IT investment. Information collected from non-DoD sources should be verified, to the extent practicable, for accuracy, that the collection is current, and the information is complete. This is especially important if the information will be used to make determinations about individuals.

17. Describe any information that is provided to an individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form.

*** Example:*

-- A Privacy Act system of records notice was published in the Federal Register with a 30 day public comment period. Forms that collect personal data will contain a Privacy Act Statement, as required by 5 U.S.C. 552a(e)(3), allowing the individual to make an informed decision about providing the data or participating in the program. Individuals may raise an objection with the Air Force Privacy Act Office during the comment period, during data collection, or at any time after the program is launched. If no objections are received, consent is presumed.

-- AFI 33-332, "Privacy Act Program", http://www.e-publishing.af.mil/pubfiles/af/33/afi33-332/afi33-332.pdf , governs Privacy Act data collections in the Air Force. AFI 33-129, "Web Management and Internet Use", http://www.e-publishing.af.mil/pubfiles/af/33/afi33-129/afi33-129.pdf discusses data collection and privacy policies. Air Force civilian employees, military members, and contractors are required to be aware of Privacy Act issues (e.g. via Privacy Act training offered by your MAJCOM/DRU/FOA/base, http://www.foia.af.mil/Privacy/Tng1.shtml , etc.) to fulfill their duties in handling third party personal data and in learning their Privacy Act rights.

18. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.

*** For these three entries, describe the controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form. Your response should provide a general description of the privacy protections and controls in place to preserve the confidentiality of the information under your control.*

Administrative:

Physical:

Technical:

19. Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11, "DoD Privacy Program," November 11, 2004. If so, and

a System Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when publication of the Notice will occur.
*** Entry will be "not applicable" for those IT investments that do not require a Privacy Act system of records notice. For those that do require a Privacy Act system of records notice, identify the notice and provide the system name. All AF Privacy Act systems of records notices are found at http://www.dod.mil/privacy/notices/usaf/ . For more information, contact the Privacy Office at your base or MAJCOM/DRU/FOA.*

20. Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures.
*** Response should indicate privacy risks unique to your IT investment. Do not provide generic language about the results of a privacy breach in general. Be specific to the risks that a privacy breach involving your IT investment and its data would generate. Do not provide specific information about the name/vendor/operating system of any security measures you identify. For example, if your IT investment consists of a Microsoft Access database, don't list the existing vulnerabilities in unpatched Microsoft Access programs. Instead, provide any vulnerabilities specific to your IT investment (e.g. lack of a username/password which can allow unauthorized users to obtain information in your Access application).*

21. State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form.
*** Classification: "Unclassified" is the common choice. If you need more information, contact your base Security Manager or reference Appendix 3 of DoD 5200.1-R, January 1997 at http://www.dtic.mil/whs/directives/corres/pdf/520001r.pdf .*
*** Publication: This document will be published either in full or in summary form on the Air Force Privacy Act website, http://www.foia.af.mil/Privacy/PrivImpAssess.shtml .*

Preparing Official (signature)
(date)
Name:
Title:
Organization:
Work Phone Number:
Email:

Information Assurance Official (signature)
(date)
Name:
Title:
Organization:
Work Phone Number:

Email:

Privacy Official (signature)
(date)
Name:
Title:
Organization:
Work Phone Number:
Email:

Reviewing Official (signature)
(date)
Name:
Chief Information Officer:
Organization:
Work Phone Number:
Email:

After the Program Manager signs the Privacy Impact Assessment as the Preparing Official and the Program Manager's Information Assurance Official (a computer professional who is familiar with the IT investment) signs off on the PIA, then the PIA and its signature page should be sent to the respective MAJCOM/DRU/FOA Privacy Act Office.

That office will review the PIA for privacy risks, concur when it is satisfied, and forward the PIA package to the AF Privacy Act Office via af.foia@pentagon.af.mil .

The Air Force Privacy Act Office will obtain the signatures of the Air Force Privacy Official and the SAF/XC Chief Information Officer (Reviewing Official), have SAF/XC Information Assurance review the PIA, publish the PIA at http://www.foia.af.mil/Privacy/PrivImpAssess.shtml , and send the PIA package to Office of the Secretary of Defense Chief Information Office (OSD CIO).

OSD CIO will perform its review and forward the package to OMB via PIA@omb.sop.gov .